

# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ  
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION  
DEPARTMENT OF TELECOMMUNICATIONS

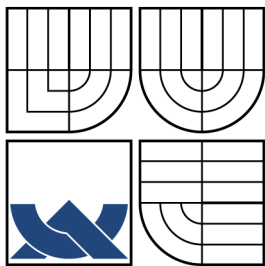
KONFIGURACE SÍTOVÝCH PRVKU V PROGRAMU  
PACKET TRACER

BAKALÁŘSKÁ PRÁCE  
BACHELOR'S THESIS

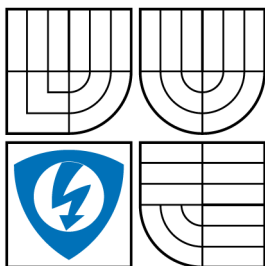
AUTOR PRÁCE  
AUTHOR

JAKUB WOLF

BRNO 2009



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ  
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY  
A KOMUNIKAČNÍCH TECHNOLOGIÍ  
ÚSTAV TELEKOMUNIKACÍ



FACULTY OF ELECTRICAL ENGINEERING AND  
COMMUNICATION  
DEPARTMENT OF TELECOMMUNICATIONS

## KONFIGURACE SÍTOVÝCH PRVKU V PROGRAMU PACKET TRACER

CONFIGURATION OF NETWORKING DEVICES IN PACKET TRACER

BAKALÁŘSKÁ PRÁCE  
BACHELOR'S THESIS

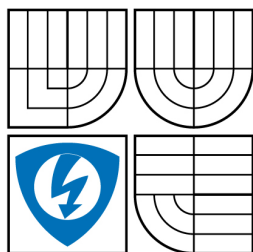
AUTOR PRÁCE  
AUTHOR

JAKUB WOLF

VEDOUCÍ PRÁCE  
SUPERVISOR

ING. DAN KOMOSNÝ, PH.D.

BRNO 2009



VYSOKÉ UČENÍ  
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky  
a komunikačních technologií

Ústav telekomunikací

# Bakalářská práce

bakalářský studijní obor  
**Teleinformatika**

**Student:** Jakub Wolf

**ID:** 70305

**Ročník:** 3

**Akademický rok:** 2008/2009

## NÁZEV TÉMATU:

### Konfigurace síťových prvků v programu Packet Tracer

#### POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s dokumenty popisující činnost a zapojení laboratoře Cisco akademie. V programu Packet Tracer proveďte konfiguraci síťových prvků laboratoře pro sadu laboratorních cvičení 2.6.2-9.8.3 kurzu CCNA1. Do síťové konfigurace zahrňte i všechny pracovní stanice laboratoře a Eagle server. Zhotovte názorné schéma vytvořené sítě a to publikujte na webových stránkách Cisco akademie ([adela.ukto.feec.vutbr.cz](http://adela.ukto.feec.vutbr.cz)). Dále v programu Packet Tracer vytvořte zadání úlohy pro sestavení vytvořené sítě. Zadání a postup vypracování úlohy popište v elearningu VUT.

#### DOPORUČENÁ LITERATURA:

- [1] GRAZIANI, R., JOHNSON, A. Routing Protocols and Concepts, CCNA Exploration Companion Guide. Cisco Press, USA, 2007. 606 s. ISBN 978-1-58713-206-3.
- [2] NEMETH, E., SNYDER, G., HEIN T. Linux - Kompletní příručka administrátora. Computer Press, 2004. 880 s. ISBN: 80-722-6919-4.

**Termín zadání:** 9.2.2009

**Termín odevzdání:** 2.6.2009

**Vedoucí práce:** Ing. Dan Komosný, Ph.D.

**prof. Ing. Kamil Vrba, CSc.**  
*Předseda oborové rady*

#### UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

## **ABSTRAKT**

Bakalárska práca sa zaoberá problematikou Cisco akademie a programom Packet tracer od firmy Cisco. Teoretická časť zameriava pozornosť na priblíženie učebne Cisco Akadémie. Nasleduje kapitola, ktorá špecifikuje operačný systém Cisco zariadení a kapitola popisujúca smerovací protokol Open Short Path First (OSPF), ktorý je použitý v praktickej časti práce. Bližšie objasňuje základné vlastnosti a fungovanie protokolu v autonómnych systémoch počítačových sietí. Praktická časť pozostáva z dvoch projektov vytvorených v programe Packet tracer. Prvý simuluje počítačovú učebnu Cisco akademie so všetkými zariadeniami. Druhý projekt predstavuje úlohu pre študentov zameranú na smerovací protokol OSPF. V závere práce sú realizované postupy zdokumentované. Súčasťou sú i webové prezentácie popisujúce oba projekty.

## **KLÍČOVÁ SLOVA**

Packet tracer, Cisco akadémia, simulácia učebne, OSPF úloha

## **ABSTRACT**

This bachelor work is concerned with a Cisco academy problem and a Packet tracer from the Cisco company. The theoretical part is orienting it's attention on approach of the Cisco Academy schoolrooms. Follows the chapter, which specifies the operating system of the Cisco equipments and chapter describing the routing protocol Open Short Path First (OSPF), which is used in a practical part of this work. It is making clear the basic characters more closely and protocol functioning in autonomous systems of computer networks. The practical part consists of two projects which are created in Packet tracer. The first one is simulating the computer schoolroom of the Cisco academy with all the equipments. The second project is introducing the homework for students which is oriented on the routing protocol OSPF. There are documented the realized progresses in fine. The part of it are web presentations which are describing both projects.

## **KEYWORDS**

Packet tracer, Cisco academy, classroom simulation, OSPF exam

WOLF, J. *Konfigurace síťových prvků v programu Packet Tracer*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 41 s. Vedoucí bakalářské práce Ing. Dan Komosný, Ph.D.

## PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Konfigurace síťových prvku v programu Packet Tracer“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne .....

.....

(podpis autora)

# OBSAH

Úvod	9
<b>1 Základy počítačových sietí</b>	<b>10</b>
<b>2 Cisco Akadémia</b>	<b>11</b>
2.1 Základný popis . . . . .	11
2.2 Počítačová učebňa . . . . .	11
2.2.1 Systém kabeláže v učebni . . . . .	11
2.2.2 Sieťové prvky umiestnené v rozvádzači . . . . .	13
2.2.3 Pracovné stanice . . . . .	13
<b>3 Operačný systém zariadení Cisco</b>	<b>15</b>
3.1 Základné vlastnosti operačného systému . . . . .	15
3.2 Ovládanie a štruktúra systému . . . . .	15
3.3 Možnosti prístupu . . . . .	16
3.3.1 Prístup cez konzolu . . . . .	16
3.3.2 Zabezpečené a nezabezpečené prístupy na tretej – sieťovej vrstve	17
3.3.3 Pomocný port . . . . .	17
<b>4 Smerovací protokol OSPF</b>	<b>18</b>
4.1 Základné informácie . . . . .	18
4.2 Metrika liniek . . . . .	18
4.3 Komunikácia medzi smerovačmi . . . . .	19
4.3.1 Spáva naviazania spojenia . . . . .	20
4.3.2 Správy s aktualizáciou smerovacej tabuľky . . . . .	21
4.4 Smerovacia tabuľka . . . . .	21
4.5 Rozdelenie sietí . . . . .	21
4.5.1 Spojenie bod–bod . . . . .	22
4.5.2 Topológia so smerovačmi v jednej sieti . . . . .	22
4.5.3 Modifikované spojenie bod–bod . . . . .	22
4.5.4 Spojenie bod–viac bodov . . . . .	23

<b>5</b>	<b>Packet Tracer</b>	<b>24</b>
<b>6</b>	<b>Vytvorenie úlohy v programe Packet tracer</b>	<b>25</b>
6.1	Formulácia požiadavkov . . . . .	25
6.2	Návrh topológie siete . . . . .	25
6.3	Postup vypracovania . . . . .	27
6.4	Tvorba doplnkových informácií a vyhodnotenia . . . . .	28
6.5	Dostupnosť úlohy . . . . .	29
<b>7</b>	<b>Vytvorenie zapojenia Cisco Akadémie</b>	<b>30</b>
7.1	Hľadanie vhodného riešenia . . . . .	30
7.2	Simulácia reálnych počítačov . . . . .	31
7.3	Stojany – racky, smerovače a prepínače . . . . .	33
7.4	Fyzické rozloženie zariadení v prostredí Packet tracer . . . . .	34
<b>8</b>	<b>Záver</b>	<b>37</b>
	<b>Literatúra</b>	<b>38</b>
	<b>Zoznam symbolov, veličín a skratiek</b>	<b>40</b>
	<b>Zoznam príloh</b>	<b>42</b>
<b>A</b>	<b>CD-ROM</b>	<b>43</b>
A.1	BP_xwolfj01.pdf . . . . .	43
A.2	cisco_class.pka . . . . .	43
A.3	cisco_exam.pka . . . . .	43
A.4	class_web.html . . . . .	43
A.5	exam_web.html . . . . .	43
A.6	styles.css . . . . .	43
A.7	Zložka: pic . . . . .	44



## ZOZNAM OBRÁZKOV

2.1	Načrtnutý pôdoris učebne Cisco akadémie. . . . .	12
2.2	Smerovač Cisco 2801. . . . .	13
2.3	Prepínač Cisco 2960-24TT. . . . .	13
6.1	Topológia vytorený pre úlohu zameranú na smerovací protokol OSPF. . . . .	26
6.2	Okno s informáciami a postupom vypracovania úlohy. . . . .	28
6.3	Dosiahnuté výsledky s detailným zobrazením jednotlivých zadání. . . . .	29
7.1	Topológia Cisco učebne s 28 počítačmi a 3 stojanmi. . . . .	31
7.2	Počítač „maskovaný“ dvoma koncovými zariadeniami. . . . .	32
7.3	Prvý stojan s prepínačom HP ProCurve a serverom. . . . .	33
7.4	Uroveň v ktorej vidieť stojany a rady. . . . .	35
7.5	Grafické znázornenie zariadení a ich zapojenia. . . . .	36
7.6	Informácie zobrazované pri každom spustení úlohy. . . . .	36

# ÚVOD

Spoločnosť Cisco je významným hráčom na celosvetovom trhu so sieťovými prvkami. Vzhľadom na jej veľký podiel sa snaží školiť ľudí, ktorí budú dostatočne kvalifikovaný na prácu s týmito zariadeniami. Preto vytvorila program nazvaný Cisco networking academy – Cisco akadémia. Program združuje autorizované centrá výuky po celom svete. Jedno z centier je aj VUT v Brne. V rámci predmetov CISCO akadémia – magisterský program (MCA) a CISCO akadémia – bakalársky program (BCA) majú študenti možnosť zúčastniť sa programu Cisco Certified Network Associate (CCNA) 1–4 zaoberajúci sa najmä základmi sietí. Cisco zároveň vyvinulo počítačový simulčný program s názvom Packet tracer. Práve s týmto programom je úzko zviazaná moja bakalárska práca.

Celá práca pozostáva z dvoch celkov – teoretickej a praktickej časti. Praktickú časť som rozdelil na dva, na sebe nezávislé projekty. Prvým projektom sa snažím premietnuť Cisco počítačovú učebňu do Packet traceru a virtuálne ju tak sprístupniť kedykoľvek študentom. Znamenalo by to napríklad, že študenti budú mať možnosť zoznámiť sa s učebňou skôr, ako v nej fyzicky začnú pracovať. Druhý projekt kladie konkrétne nároky na prácu študenta v simulácii. Vytvoril som úlohu zameranú na smerovací protokol Open Short Path First (OSPF). Študent bude mať za úlohu dokončiť implementáciu smerovacieho protokolu na mnou pripravenej topológii. V kapitolách 6 a 7 sa snažím zrozumiteľnou formou popísať postup a úskalia späté s projektami.

V teoretickej časti zameriavam pozornosť na základné vlastnosti operačného systému Cisco Internetwork Operation System (IOS) (kap. 3) a najmä na smerovací protokol OSPF (kap. 4), ktorý je použitý v praktickej časti práce. Snažil som sa vysvetliť základné aspekty fungovania v sieťach s implementovaným smerovacím protokolom OSPF. Poznatky z tejto kapitoly slúžia ako teoretická príprava na úlohu zpracovanú v praktickej časti.

Prácu som sa snažil podať zrozumiteľne aby bolo jej výsledok, simuláciu učebne a úlohu pre študentov, možné publikovať v e-Learningu VUT. Pre tieto účely som vytvoril webovú prezentáciu.

# 1 ZÁKLADY POČÍTAČOVÝCH SIETÍ

Výraz počítačová sieť označuje súbor viacerých počítačov a sieťových prvkou, medzi ktorými sú vytvorené informačné kanály. Tie vo väčšine majú formu fyzického spojenia pomocou káblov. Dôležitou časťou sú už spomínané sieťové prvky. Triedenie týchto zariadení do skupín prebieha na základe toho, na akej vrstve Open Systems Interconnection (OSI) modelu pracujú. OSI model reprezentuje univerzálny referenčný model, riadiaci komunikáciu medzi prvkami siete bez ohľadu na použitú technológiu [11]. Pre potreby niektorých komunikačných protokolov vznikli transformované modely s rozdielnym počtom vrstiev. Medzi základnými prvkami siete figurujú tieto zariadenia:

- Hub – rozbočovač operuje na fyzickej vrstve, ktorá je v rámci referenčného modelu OSI najnižšie. Neobsahuje žiadne sofistikované riadenie preposielania správ. Ide o jednoduché kopírovanie na všetky rozhrania.
- Switch – prepínač pracuje na druhej tzv. spojovej vrstve. Prepínač posíla správa na konkrétne rozhranie. Rozhoduje na základe cieľovej adresy sieťovej vrstvy.
- Router – smerovač hraje úlohu hraničného bodu medzi sieťami, líšiacich sa v tretej – sieťovej vrstve. Pole pôsobnosti je, na rozdiel od predchádzajúcich prvkou, zpravidla mnohonásobne väčšie [8].

Smerovače a prepínače tak ako každý iný komplikovanejší prístroj potrebuje operačný systém ktorý má na starosti sprostredkovať komunikáciu medzi užívateľom a zariadením. Zvládnutie takéhoto systému je základ pri administrácii siete.

## 2 CISCO AKADÉMIA

### 2.1 Základný popis

Cisco Akadémia sa vyučuje ako voliteľný všeobecne vzdelávací predmet pod záštitou Ústavu telekomunikácií na VUT v Brne. Jeho cieľom je príprava na certifikát CCNA. Vyučuje sa od zimného semestra akademického roku 2007/2008. Výuka prebieha na bakalárskom aj na magisterskom stupni. Celá náplň je rozdelená do dvoch semestrov. Každý jeden semester je rozdelený do dvoch tematických častí.

V prvom semestri to sú CCNA1 a CCNA2. Celok CCNA1 je zameraný na priblíženie základnej problematiky sieťového hardware a zoznámenie sa s Transmission Control Protocol / Internet Protocol (TCP/IP) protokolovou sadou. CCNA2 obsahuje informácie o smerovacích protokoloch používaných v smerovačoch.

Letný semester zoznamuje v prvej časti so základnými a pokročilými nastaveniami prepínačov a v druhej približuje problematiku reálnych sieťových aplikácií a základných prostriedkov pre komunikáciu v rámci metropolitných sietí a Internetu. Kurzy prebiehajú v českom jazyku. Materiály v anglickom jazyku sú natívne poskytované Cisco Systems a prístupné na oficiálnej internetovej stránke po prihlásení.

### 2.2 Počítačová učebňa

#### 2.2.1 Systém kabeláže v učebni

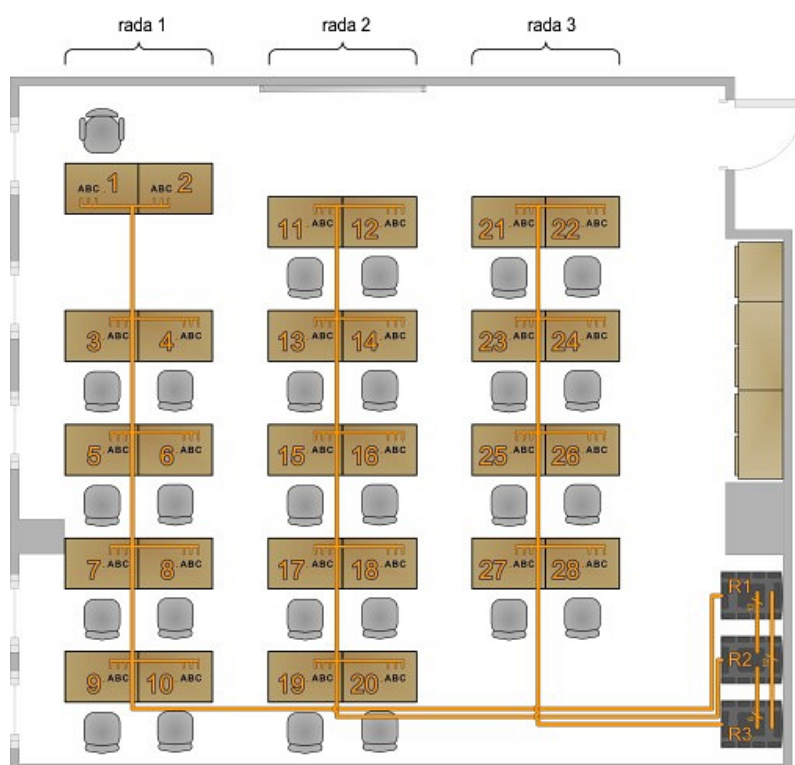
Miestnosť pre výuku predmetov BCA a MCA je situovaná v najnižšom poschodí budovy VUT na ulici Purkyňova 118 v Brne. V miestnosti sa nachádza 26 pracovných staníc. Rozloženie je zrejmé z obr. 2.1. Každý obsahuje dve sieťové karty. Jedna zabezpečuje pripojenie do ostrej siete VUT a Internetu [1]. Internet Protocol (IP) adresy sú z verejného rozsahu 147.229.0.0/16 pridelené Dynamic Host Configuration Protocol (DHCP)<sup>1</sup> severom. Druhá zo sieťových kariet, ktorú počítač obsahuje, slúži pre prístup do testovacej siete. Každá stanica má okrem toho pripojený kábel

---

<sup>1</sup>Protokol na automatické pridelenie IP adres sieťovým prvkom [4]

RJ45-DB9. Je to tzv. rollover kábel. Na strane počítača je zapojený do sériového portu a na druhej má zásuvku pre koncovku RJ45. Slúži pre prístup na konzolu prepínačov a smerovačov. Celkovo sa v miestnosti nachádzajú tri rozvádzače. Pre každú radu jeden.

Do každého jedného rozvádzača sú z počítačov vyvedené už spomínané sieťové karty a sériový port, označené číslami (1-26) a písmenami (A, B, C, D). Číslo jednoznačne označuje pracovnú stanicu a písmená príslušnú kartu alebo vyvedený sériový port. Karta určená na laboratórne úlohy má písmeno C. Port určený pre konzolu písmeno B. Manipulácia s týmito zásuvkami je plne v rukách študenta. Výnimku tvoria porty A umiestnené v rozvádzači R1. Na tieto porty sú privedené káble zo sieťových kariet, určených pre ostrú prevádzku. Spojenie ďalej vedie do prepínača HP ProCurve a následne do Internetu. S touto časťou rozvádzača majú študenti zakázanú manipuláciu. Port s označením D zabezpečuje prístup do záložnej siete a vo výuke sa nepoužíva [1].



Obr. 2.1: Načrtnutý pôdoris učebne Cisco akademie.

Štandardne pracuje každá rada na vlastnom rozvádzači. V dôsledku obmedzeného

množstva prepínačov a smerovačov v rozvádzačoch, je niekedy nutné prepojiť prvky v rôznych rozvádzačoch medzi sebou. K tomu slúžia dátové cesty medzi rozvádzačmi. V celej učebni je použitá kabeláž kategórie 5.

### 2.2.2 Sieťové prvky umiestnené v rozvádzači

V miestnosti sú k dispozícii nasledujúce prvky od Cisco Systems: 18x smerovač Cisco 2801 (obr. 2.2) a 13x prepínač Cisco Catalyst 2960-24TT (obr. 2.3).



Obr. 2.2: Smerovač Cisco 2801.



Obr. 2.3: Prepínač Cisco 2960-24TT.

### 2.2.3 Pracovné stanice

V učebni je k dispozícii 26 počítačov HP dc7700 SFF, ktoré obsahujú pripravené obrazy pracovných operačných systémov. Základným systémom je Linux kde má študent najmenšie práva z dôvodu, či už úmyselných, alebo náhodných zmien v nastavení sieťovej karty zapojenej do ostrej siete VUT [1].

V hlavnom operačný systém (OS) je nainštalovaný virtualizačný softvér VMware, ktorý sprostredkováva úplnú virtualizáciu. To znamená, že spustí operačný systém

fungujúci paralelne so základným, ale na iných úrovniach. Základný pracuje priamo na hardvéri a vytvára druhému systému virtuálny hardvér. Virtuálny systém takúto zmenu nespozná a preto pracuje ako by bol práve on ten základný. Sieť funguje na princípe smerovača s Network Address Translation (NAT)<sup>2</sup>, kde túto úlohu hraje základný operačný systém.

Na výber sú dva operačné systémy: Windows XP a Linux, ktoré možno spúšťať podľa znalostí a schopností študenta. Samozrejme nie je problém pridať ďalší operačný systém. O takúto zmenu sa však stará správca siete. Virtuálne systémy majú výhodu vo svojej nezničiteľnosti. Ani poškodenie nekorektnou inštaláciou a následným odstránením softvéru nemá nevratný charakter. Riešenie virtuálnymi systémami uľahčuje správu počítačov.

---

<sup>2</sup>Protokol používaný pri preklade IP adres a portov pri prechode cez smerovač [8]

## 3 OPERAČNÝ SYSTÉM ZARIADENÍ CISCO

Vzhľadom na skutočnosť že sieťové prvky predstavujú určitý druh počítača, potrebujú operačný systém, ktorý bude predstavovať most medzi užívateľom a samotným zariadením. Výnimkou nie sú ani zariadenia od firmy Cisco. Pretože práve zládnutie tejto problematiky predstavuje základ k úspešnému dokončeniu počítačových úloh, považujem za dôležité sa zmieniť o základných vlastnostiach a špecifikáciách operačného systému v prvkoch Cisco.

### 3.1 Základné vlastnosti operačného systému

V Cisco prvkoch tvorí most medzi užívateľom a hardvérom operačný systém IOS. V určitých modifikáciách ho obsahuje každý Cisco prepínač, smerovač, HUB, Wireless Fidelity (Wi-Fi) prístupový bod a veľa ďalších. Medzi funkcie poskytované IOS patria:

- základné prepínacie a smerovacie funkcie,
- spoľahlivosť a bezpečnosť,
- adaptabilnosť na zmeny v sieti.

### 3.2 Ovládanie a štruktúra systému

IOS je modálny operačný systém s hierarchickou štruktúrou ovládacích módov. V poradí od najnižšieho po najvyšší mód to sú tieto:

- základný mód (User executive Mode),
- privilegovaný mód (Privileged executive mode),
- globálny konfiguračný mód (Global configuration mode),
- iné špecifické konfiguračné módy (Other specific configuration modes) [7].



Za hlavnú výhodu hierarchického systému je treba vyzdvihnúť jeho bezpečnostnú stránku. Používajú sa rôzne druhy autentifikácií pre rôzne módy.

Ovládanie celého systému prebieha cez príkazový riadok Command-line interface – príkazový riadok (CLI), alebo zriedkavo používané webové rozhranie. Každý mód implementuje iné nastavenia a každý obsahuje vlastnú sadu príkazov. Príkazy potrebujú špecifickú syntax, ktorú treba dodržiavať.

### 3.3 Možnosti prístupu

Na každý sieťový prvok existuje viacero druhov prístupov, avšak medzi najpoužívanejšie patria:

- konzola,
- telnet<sup>1</sup> (Telecommunication Network), alebo Secure Shell (SSH)<sup>2</sup>,
- Auxiliary – pomocný port (AUX) – pomocný port [7].

#### 3.3.1 Prístup cez konzolu

Tento typ prístupu je charakterizovaný tým, že užívateľ je priamo pripojený k smerovaču, alebo prepínaču pomocou úzko pásmovej sériovej linky. Používaný je najmä pri prvotnej konfigurácii, keď ešte nefunguje, alebo je obmedzená sieť tretej sieťovej vrstvy OSI. Ďalej napríklad za účelom obnovenia hesla z dôvodu jeho straty, alebo podobnej výnimočnej udalosti. Zariadenie implicitne neaplikuje na tento port žiadne zabezpečenie, avšak je možné a malo by byť použité, za účelom ochrany proti neautorizovanému prístupu.

---

<sup>1</sup>Protokol pracujúci na aplikačnej vrstve. Ovláda zariadenia v sieti cez terminál s príkazovým riadkom [8].

<sup>2</sup>Protokol umožňujúci bezpečnú komunikáciu medzi počítačmi pomocou šifrovania [8].

### **3.3.2 Zabezpečené a nezabezpečené prístupy na tretej – sieťovej vrstve**

Je to metóda používajúca vzdialený prístup k zariadeniu. Aby pripojenie bolo uskutočniteľné, je potrebné, aby na smerovači bol nastavený najmenej jeden port s funkčnou adresou tretej vrstvy OSI, ako napríklad Internet Protocol version 4 (IPv4). Z bezpečnostných dôvodov je tento prístup primárne zakázaný. Na aktiváciu postačuje zadať prístupové heslo. Cisco zariadenia obsahujú aj telnet klienta, ktorý môže byť použitý na konfiguráciu iného smerovača alebo prepínača. Na rozdiel od telnetu obsahuje SSH vo svojej špecifikácii vylepšené bezpečnostné prvky, napríklad šifrovaný prenos dát medzi klientom a serverom. Z tohto dôvodu je preferované používať tento typ prístupu. Tak ako v prípade telnetu, v IOS je možné používať zariadenie ako SSH klienta, alebo SSH server.

### **3.3.3 Pomocný port**

Ďalším spôsobom, ako naviazať spojenie je pomocou vytáčaného pripojenia na AUX porte. Rovnako, ako v prípade konzolového prístupu, aj tu sa použitie odvíja od predpokladu, že na smerovači nebeží žiadna sieťová služba a nie je na ňu možné pristupovať vzdialene.

## 4 SMEROVACÍ PROTOKOL OSPF

Časť mojej bakalárskej práce sa zaoberá smerovacím protokolom OSPF. Preto považujem za nutné sa o ňom v krátkosti zmieniť.

### 4.1 Základné informácie

Smerovací protokol OSPF začal vznikať v roku 1987 v rámci projektu globálnej počítačovej siete, Internetu, ktorú v tej dobe ešte zastrešovala americká vláda a organizácia The Internet Engineering Task Force (IETF). V súčasnosti sa používa vo verzii Open Short Path First version 2 (OSPFv2) [9].

OSPF je predstaviteľ protokolu, ktorý mení informácie uložené v smerovacej tabuľke na základe zmeny v sieti a zaraďujeme ho do skupiny Interior Gateway Protocol (IGP). To znamená, že je určený k používaniu v rámci jedného autonómneho systému. Každý smerovač si udržiava kompletnú mapu – topológiu, siete v databáze. Nad touto databázou pracuje algoritmus označovaný Shortest Path First (SPF), ktorého úlohou je vypočítať najlepšiu cestu do cieľovej siete. OSPF má výhodu oproti starším smerovacím protokolom (Routing Information Protocol (RIP)), že je ho možné použiť na relatívne veľké siete. Hierarchické usporiadanie znižuje nároky na výpočetnú kapacitu a sieť samotnú. Sieť je rozdelená na oblasti (area). Link State Advertisement (LSA) pakety sa šíria iba tej danej oblasti a tiež výpočet SPF algoritmu sa spúšťa pre každú oblasť zvlášť. Medzi oblasťami sa posielajú sumarizované informácie. Zmena topológie v jednej oblasti nemá dopad na výpočet SPF algoritmu v ostatných oblastiach [2].

### 4.2 Metrika liniek

Ako každý smerovací protokol tak aj OSPF potrebuje rozhodovací mechanizmus, na základe ktorého, bude určovať ktorá cesta je pre paket najvýhodnejšia. Staršie protokoly, napríklad RIP, používal jednoduchý parameter – počet preskokov, to znamená koľko smerovačov musí paket prejsť, aby dorazil do cieľa. Toto číslo je obmedzené na

16, čo je možno považovať za nevýhodu [3]. Na rozdiel od tohto systému porovnávania výhodnosti ciest, OSPF využíva sofistikovanejší algoritmus na výber najlepšej cesty. Parameter, označovaný ako cena (cost), je číslo ktoré nadobúda hodnoty od 1 do 65535, priradené každému rozhraniu smerovača. Čím menšie číslo, tým má cesta lepšiu metriku a je teda viac preferovaná. Implicitne má každé rozhranie priradenú cenu automaticky na základe šírky pásma daného rozhrania podľa vzťahu [9]:

$$cena = 100000000 / < rychlostlinky > [b/s]. \quad (4.1)$$

Aby všetko fungovalo bez problémov, je treba správne nastaviť šírku pásma. Ako je vidieť, linky FastEthernet majú cenu 1, preto niektoré OSPF implementácie dovoľujú zmeniť konštantu 100 000 000 na väčšie číslo. Tak isto je možné zmeniť metriku ručne pre prípad, že by bolo nutné využívať jednu linku viac, ako druhú. Výsledná cena cesty do cieľa je daná súčtom všetkých liniek na ceste k cieľu.

## 4.3 Komunikácia medzi smerovačmi

Komunikácia v oblasti OSPF prebieha pomocou IP paketov s číslom protokolu 89 na jednej z dvoch viac-smerových (multicast) adries 224.0.0.5, alebo 224.0.0.6. Na Ethernet linke je, ako každý iný paket, zabalený do Ethernet rámca s viac-smerovými adresami 01-00-5E-00-00-05, alebo 01-00-5E-00-00-06. Číslo Time To Live (TTL)<sup>1</sup> je nastavené na 1 čo zaručuje, že správy neputujú ďalej, ako jeden smerovač. Komunikáciu OSPF zabezpečujú Link State Packets (LSP). Každý paket má špecifickú funkciu.

**HELLO** – jedná sa o správu ktorá je vyslaná ako prvá, aby smerovač dal vedieť o svojej existencii aj ostatným.

Database Description (DBD) — kontroluje synchronizáciu databáz v zariadeniach.

Link State Request (LSR) — požiadavka slúžiaca smerovaču v prípade, keď považuje uchované informácie za staré alebo chybné.

---

<sup>1</sup>Číslo v hlavičke paketu, ktoré sa automaticky zníži prechodom uzla. Keď klesne na nulu je paket zahodený [8]

Link State Update (LSU) — odpoveď na LSR. Obsahuje požadované informácie o sieťach.

Link State Acknowledgement (LSAck) — smerovač ktorý prijme LSU packet odpovedá LSAck správou, aby dal na vedomie, že správu spracoval. V prípade, že smerovač posielajúci LSU nedostane LSAck, opakuje vysielanie po uplynutí časového intervalu [2].

### 4.3.1 Spáva naviazania spojenia

Skorej ako si budú smerovače vymieňať smerovacie informácie, je treba nájsť susedov a naviazať s nimi spojenie. Použije k tomu HELLO správu ktorú periodicky posielá na každé rozhranie, ktoré má definovaný smerovací protokol OSPF. HELLO pakety sú používané na:

- nájdenie susedov,
- rozhlasovanie parametrov s akými bude spojenie naviazane. Musia s nimi súhlasiť oba smerovače,
- zvolenie Designated Router – referenčný router (DR) a Backup Designated Router – záložný referenčný router (BDR) vo viac prístupových sieťach (multiaccess) sieťach ako napríklad Ethernet [2].

Nutnosťou je, aby pri komunikácii mal každý svoju jedinečnú adresu, respektíve identifikačné číslo. Toto číslo, ID smerovača (Router ID), ma hodnotu najvyššej IP adresy spätnej slučky (loopback) na smerovači. Pokiaľ nie je rozhranie nakonfigurované, berie sa do úvahy najvyššia IP adresa ľubovoľného rozhrania. HELLO pakety sú posielané s intervalom HelloInterval, ktorý má v Local Area Network (LAN) sieťach štandardne hodnotu 10s. Pokiaľ smerovač nedostane od svojho suseda HELLO správu za čas dlhší ako je nastavený (DeathInterval), považuje tohto suseda za nefunkčného a vymaže ho zo svojej Link-State databázy. Implicitne je vo viac-prístupových (multiaccess) a bod-bod (Point-to-Point) sieťach DeathInterval dlhý 40s. Pre siete bez viac-smerovej komunikácie Non-Broadcast Multiple Access (NBMA) platí hodnota 120s [9].

Ďalší nutný parameter, ktorý má význam najmä vo viac-prístupových sieťach, je zvolenie referenčného smerovača DR a záložného BDR. DR zariadenie radi v sieti aktualizácie, z dôvodu zníženia zaťaženia siete prebytočnými dátovými tokmi z ostatných smerovačov. V bod-bod spojeniach nemá zvolenie referenčného bodu význam. K dohode strán nastáva v prípade, že parametre ako HELLO Interval, DeathInterval, číslo oblasti (Area ID) a typ siete (Network type) sa zhodujú [6].

### 4.3.2 Správy s aktualizáciou smerovacej tabuľky

Sú to správy ktoré zabezpečujú samotnú distribúciu informácií. Každá LSU aktualizácia obsahuje niekoľko LSA. Po tom čo si smerovače navzájom vymenia svoje databázy, skontrolujú kompletnosť údajov. V prípade negatívneho výsledku požiadajú suseda o znovu prenesenie informácií. Správy sa šíria po sieti zo smerovača na smerovač. Každý paket je treba potvrdiť. Slúžia na to pakety typu LSAck. Pokiaľ sa správa nedorazí po vypršaní intervalu je posielaná znova.

## 4.4 Smerovacia tabuľka

Dôležitou súčasťou celého systému, je premena vstupnej databázy na smerovaciu tabuľku pomocou algoritmu. Celú databázu môžeme interpretovať ako graf, popisujúci štruktúru siete s odpovedajúcou metrikou. SPF algoritmus nájde najekonomickejšiu cestu a vylúči všetky sľučky. Z celej vypočítanej cesty sa vo finále použije adresa prvého smerovača na ceste (next hop) a sumár ceny pre túto cestu. Reálne môže nastať situácia, že do cieľovej siete vedie niekoľko ciest s rovnakou cenou. Konflikt rieši smerovač vybraním jedenej, alebo rozložením záťaže na všetky uvedené. Výpočet SPF algoritmu predstavuje záťaž a je žiaduce, aby neprebíhal príliš často. K tomu dôjde v prípade nestabilnej linky, ktorá alternuje medzi stavmi zapnutá, vypnutá. Dôležitý krok, je zavedený časový interval medzi jednotlivými výpočtami [6].

## 4.5 Rozdelenie sietí

V sieti spravovanej OSPF smerovacím protokolom definujeme päť rôznych typov:

- Point-to-point,
- Broadcast Multiple Access,
- Non-Broadcast Multiple Access,
- Point-to-multipoint,
- Virtual links [3].

#### 4.5.1 Spojenie bod–bod

Point-to-point definuje spojenie medzi dvoma smerovačmi. Typickým príkladom je sériová linka. Nie je volený žiadny DR ani BDR a smerovače sa stávajú vždy príslušnými. Komunikácia prebieha na multicast adrese 224.0.0.5

#### 4.5.2 Topológia so smerovačmi v jednej sieti

Ako broadcast siete označujeme tie, ktoré sú schopné navzájom prepojiť viacej, ako jedno zariadenie a paket vyslaný stanicou môže prijímať súčasne viacero počítačov. Typickým príkladom je Ethernet. Keby smerovače postupovali pri komunikácii, ako v Point-to-Point sieťach, režia v sieti by sa exponenciálne zvyšovala s počtom zariadení. Preto je jeden smerovač poverený do funkcie DR. Po zvolení DR a BDR prebieha celá OSPF komunikácia cez tento bod. Poverený smerovač reprezentuje celý segment siete navonok a iba on posíla informácie do ostatných segmentov siete. Porucha DR má za následok posunutie BDR smerovača o úroveň vyššie na DR a voľbu nového BDR. Komunikácia prebieha na dvoch viac-smerových adresách. Prvú 224.0.0.5 používajú všetky smerovače a druhú 224.0.0.6 iba DR a BDR.

#### 4.5.3 Modifikované spojenie bod–bod

Prípad siete, ktorá umožňuje zapojiť viac smerovačov, ale neumožňuje broadcast komunikáciu. Preto majú zariadenia problém nájsť susedov. Riešenie predstavuje implementácia do nastavení pri inicializácii a zaistiť, aby DR smerovač mal možnosť komunikovať so všetkými smerovačmi zaradenými do OSPF topológie.

#### **4.5.4 Spojenie bod–viac bodov**

Špeciálny prípad, keď je NBMA sieť chápaná ako súhrn point-to-point liniek. DR a BDR sa nevolí.



## 5 PACKET TRACER

Celú svoju prácu som vytváral v programe Packet tracer. Jedná sa o simulačné prostredie vyvinuté na edukačné účely pre Cisco Networking Academy program. Aktuálne vychádza vo verzii 5.1 . Pre Cisco študentov je voľne stiahnuteľný na Cisco stránkach. Packet Tracer je multiplatformový program, ktorý funguje ako pod Windowsom, tak aj pod Linuxom.

Užívateľsky prívetivé prostredie prináša možnosti vytvárania vlastnej topológie siete, nastavenia prvkov a následné testovanie. Prvky sú rozdelené do niekoľkých skupín podľa ich funkcie. Od smerovačov, prepínačov, Wi-Fi prístupových bodov až po užívateľské stanice a servery. V prípade Cisco prvkov je samozrejmosť konfigurácie cez CLI, prípade cez kontextové menu. Nastavenie staníc prebieha cez menu a poskytuje základné služby, ako webový prehliadač, terminál a dôležitý príkazový riadok odvodený od Windows. Obsahuje najčastejšie príkazy používané v spojení so sieťovými službami, napríklad ping<sup>1</sup>, tracer<sup>2</sup>, Address Resolution Protocol (ARP)<sup>3</sup>, telnet, ssh a ďalšie [10]. Voľba kabeláže medzi zariadeniami závisí od užívateľa. Ten vyberá medzi automatickou voľbou, alebo podľa svojich znalostí volí konkrétnu.

Packet tracer obsahuje zaujímavý nástroj Activity wizard. Rozširuje program o nové možnosti zamerané najmä na tvorbu úloh [10]. To znamená, že napríklad študent dostane súbor s pripravenou topológiou a zároveň aj informácie o zadaniach jednotlivých podúloh a kontrolu správnosti. Študent má okamžitú kontrolu nad tým, čo spravil správne a čo nie. A práve cez nadstavbu Activity wizard sa tieto vlastnosti úlohy nastavujú a programujú. V tomto nástroji som vytváral simuláciu Cisco akademie a aj úlohu pre študentov.

---

<sup>1</sup>Preveruje funkčnosť spojenia medzi dvoma sieťovými rozhraniami [8].

<sup>2</sup>Vypisuje uzly na ceste paketu od zdroja k cieľu. Uzly zisťuje pomocou zvyšujúcej sa hodnoty TTL v hlavičke [8].

<sup>3</sup>Slúži na zisťovanie páru Media Access Control (MAC) adresa – IP adresa [3].

## 6 VYTVORENIE ÚLOHY V PROGRAME PACKET TRACER

Cieľom tejto časti bakalárskej práce bolo vytvoriť úlohu, zameranú na jednu konkrétnu tému vychádzajúcu z predmetov MCA a BCA. Výsledok má formu súboru stiahnuteľného z eLearningu a spustiteľného programom Packet tracer.

### 6.1 Formulácia požiadavkov

Prvý krok pri vypracovaní, bol nájsť správnu oblasť na ktorú sa má daná úloha zameriavať. Za cieľ som si kládol vybrať tak, aby vo výsledku zahrňovala v čo možno najväčšej miere technológie, s ktorými je študent často v kontakte a ktorých zvládnutie predstavuje faktor, zohrávajúci kľúčovú úlohu pri zvládnutí celého predmetu. Zároveň som kládol dôraz na to, aby úloha obsahovala postupy, ktorých zvládnutie nie je náročné, ale významné. Takúto činnosť zahrňuje napríklad základnú konfiguráciu sieťovej karty na počítači a konfiguráciu rozhraní aktívnych prvkov. Po posúdení všetkých požiadavkov som sa rozhodol zamerať na smerovací protokol OSPF (kapitola 4). Splňuje všetky podmienky stanovené na začiatku. Snažil som sa obsiahnuť všetky možnosti, popísané v kapitole 4.5. A ako už bolo povedané, asi 20 % úlohy je spojených so základnou konfiguráciou bežných zariadení. Vo finále by študent mal zvládať nastaviť OSPF protokol na Cisco smerovačoch v rôznych zapojeniach.

### 6.2 Návrh topológie siete

Ďalším logickým krokom je tvorba topológie siete, na ktorej bude smerovací protokol OSPF konfigurovaný. Úloha mala jasný cieľ predstaviť hlavné možnosti OSPF. Týmto sa musela riadiť aj topológia, ktorá v sebe zahŕňať rôzne druhy prepojení smerovačov. Po dôkladnom zvážení padlo rozhodnutie, že topológia musí obsahovať minimálne päť smerovačov a dostatočný počet koncových staníc, ktorých presný počet však nezohráva kľúčovú úlohu. Prítomnosť prepínačov nutná nie je, ale jejich

The diagram illustrates a network topology with three routers (R1, R2, R3) forming a triangle. The links between the routers have the following speeds: 128kbps between R1 and R2, 64kbps between R1 and R3, and 256kbps between R2 and R3. The network is divided into several subnets and connected to various devices:

- Subnet 10.0.4.0/29:** Connected to R1 and R2. Includes PC6 (172.10.1.1/28) and R5 (172.10.1.1/28).
- Subnet 172.10.0.1/28:** Connected to R1 and R2. Includes PC5.
- Subnet 172.30.15.0/28:** Connected to R2 and R3. Includes PC4.
- Subnet 10.0.1.0/30:** Connected to R1 and R2.
- Subnet 10.0.2.0/30:** Connected to R2 and R3.
- Subnet 10.0.3.0/30:** Connected to R1 and R3.
- Subnet 172.10.15.0/28:** Connected to R1. Includes PC1 and PC2.
- Subnet 172.20.15.0/28:** Connected to R3. Includes PC3.

smerovačov, päť prepínačov a šesť pracovných staníc. Packet tracer ponúka viacero typov zariadení, ktoré sa líšia programovým vybavením (ponúkané funkcie), alebo hardvérom (počet a typy rozhraní). Vzhľadom na skutočnosť, že sa jedná o protokol OSPF, tak nebolo nutné hľadiť na funkcie, ktoré smerovač ponúka, pretože je to štandard u všetkých dostupných smerovacích zariadení. Dôležitejšiu úlohu zohrávali rozhrania. Pre výber smerovača sa ako najvýhodnejšie javil typ C2620. Tento typ je dostačujúci pre smerovače R4 a R5. Pre ostatné – R1, R2, R3 však potrebuje upraviť pomocou rozširovacích modulov. Použil som dva a to konkrétne 2–krát modul s dvoma sériovými linkami a jeden s dvoma rozširujúcimi FastEthernet rozhraniami. Tým som dosiahol stavu, kedy je možné bez problémov pripojiť dve siete, ktoré sa budú oznamovať cez protokol OSPF.

26

medzi smerovačmi zabezpečujú najmä sériové linky, je toto riešenie názornejšie.

## 6.3 Postup vypracovania

Cieľom úlohy je teda konfigurácia smerovacieho protokolu OSPF na všetkých smerovačoch. Nie je to však jediná časť, ktorá je nutná k úspešnému dokončeniu. Okrem iného, je nutné správne nakonfigurovať koncové zariadenia – počítače a na smerovači R1 aj jeho sériové a ethernetové rozhrania. Študent začína práve týmto krokom. Nastavovanie takeého množstva počítačov by však bolo zdĺhavé a z hľadiska výukového aj zbytočné. Z toho dôvodu stačí konfigurovať iba počítače PC1, PC2 a už spomínaný smerovač R1.

Postup je klasicky, cez kontextové menu v prípade počítačov a príkazový riadok používaný v smerovačoch popísaný v kapitole 3. Celý proces je skomplikovaný správnym zvolením IP adries, ktoré je nutné dopočítať. Ostatným zariadeniam som základnú konfiguráciu nastavil. Tým práce na prípravách k implementovaniu samotného smerovacieho protokolu OSPF skončila.

OSPF sa na smerovačoch aktivuje klasicky cez CLI pomocou príkazov v globálnom konfiguračnom móde. Je dobré kontrolovať správnosť príkazov v aktuálnu smerovaciu tabuľku. Z nej jasne vypláva, či protokol pracuje správne, teda či správne analyzuje prichádzajúce informácie o ostatných sieťach a taktiež, či ďalej posiela bezchybné informácie. Najjednoduchšie prebieha konfigurácia na smerovačoch R1, R2 a R3. Jedná sa totiž o spojenia bod–bod (kapitola 4.5.1).

Iná situácia nastáva v sieti medzi smerovačmi R4, R5 a jedným rozhraním R2. Figuruje tu prepínač, ktorý nedelí úsek medzi smerovačmi na siete, s rozdielnou adresou. To znamená, že hovoríme o viac smerovom spojení (kapitola 4.5.2). V tejto chvíli by mal smerovací protokol OSPF fungovať bez problémov na všetkých smerovačoch. Kontrola prebieha cez smerovacie tabuľky, alebo príkazom ping na staniaciach a smerovačoch. V prípade nezdaru je samozrejmé nutné nájsť chybu a odstrániť ju.

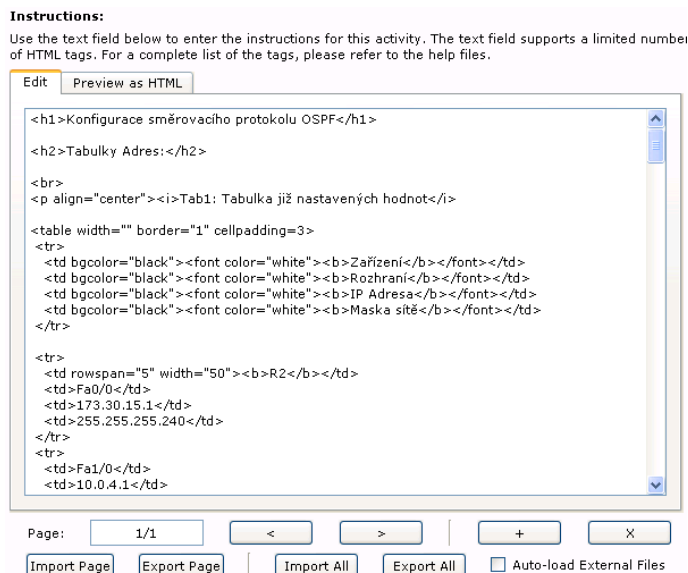
Nasleduje časť zameraná na doladenie fungujúceho systému. Najskôr upravujeme parametre vo viac smerovej sieti. Ladenie spočíva v zmene DB smerovača. Cieľom je donútiť smerovač R2, aby sa vzdal postu DB smerovača a prenechal ho jednému

z dvojice R4, R5. Realizácia prebieha v konfigurácii spätnej slučky rozhrania na už spomýnanej dvojici.

Scénar druhej časti zameriava svoju pozornosť na nastavenie rýchlostí liniek medzi smerovačmi R1, R2, R3. Výsledný efekt sa prejaví na zmene cesty, ktorú pakety pocestujú. Rýchlosti sú zrejmé z obrázku. Z fungovania OSPF protokolu vypláva, že takýto zámer je realizovateľný dvoma spôsobmi: priamou editáciou rýchlostí na rozhraní, alebo nastavením ceny linky v kontextovom menu OSPF. Týmto boli vyčerpané všetky zadania úlohy.

## 6.4 Tvorba doplnkových informácií a vyhodnotenia

Celou úlohou sprevádza návod, ktorý som naprogramoval do druhého okna spusteného spolu s úlohou (obr. 6.2). V okne sú okrem iného aj informácie o cieľoch, použitých IP adresách, príkazoch a ďalšie dôležité údaje. Nástrojom na formátova-



Obr. 6.2: Okno s informáciami a postupom vypracovania úlohy.

nie textu je značkovací jazyk HTML so základnými značkami – tagmi. Informácie nie sú jedným údajom v okne. Zaznamenáva sa čas od štartu po koniec. Úspešný

koniec nastáva v stave, keď je splnená na 100%. To znamená že všetko bolo dokončené správne. Kritéria podľa ktorých sa jednotlivé časti hodnotia a bodujú som nastavil podľa obtiažnosti zadanií. Všetky sú zobrazené v správe po ukončení úlohy (obr. 6.3). Návrat na topológiu a opravu chýb nie je problém.

Activity Results

Time Elapsed: 00:00:14

You did not complete the activity. Please close this window and try again.

Overall Feedback

Assessment Items

Connectivity Tests

Assessment Items

Status

Points

Component(s)

Feedback

Network

PC1

Ports

FastEthernet

IP Address

Incorrect1

IP adresa

Subnet Mask

Incorrect1

Maska

PC2

Default Gateway

Incorrect1

Výchozí brána

Ports

FastEthernet

IP Address

Incorrect1

IP adresa

Subnet Mask

Incorrect1

Maska

R1

Console Line

1

Physical

Password

Incorrect2

Heslo pro přístup přes konzolu

Enable Secret

Incorrect2

Zašifrování hesel

OSPF

Process ID 1

Incorrect2

Area

Area 1

Area Status

Incorrect1

Nastavení OSPF oblasti

Virtual Link

Incorrect1

Nastavení OSPF oblasti

Networks

10.0.1.0 255.255.255.252 area1

Incorrect2

Síť určená pro směrování

10.0.0.0 255.255.255.252 area1

Incorrect2

Síť určená pro směrování

172.10.15.0 255.255.255.240 ...

Incorrect2

Síť určená pro směrování

172.10.15.16 255.255.255.240 ...

Incorrect2

Síť určená pro směrování

Total Points : 0

Completed Items : 0

Required Items : 61

Component

Correct/Total Points

Clock rate

0/1 0

Heslo pro přístup přes konzolu

0/1 0

IP adresa

0/10 0

Maska

0/9 0

Nastavení OSPF oblasti

0/10 0

Other

0/4 0

Routing

0/3 0

Rozhraní bez OSPF správy

0/6 0

Síť určená pro směrování

0/14 0

Výchozí brána

0/1 0

Zašifrování hesel

0/1 0

Obr. 6.3: Dosiahnuté výsledky s detailným zobrazením jednotlivých zadanií.

## 6.5 Dostupnosť úlohy

Úloha by mala byť prístupná cez e-Learning VUT. Je vo forme súboru pre program Packet tracer 5.1. Vytvoril som aj webovú prezentáciu, ktorá vysvetľuje základné princípy práce v simulačnom prostredí.

## 7 VYTVORENIE ZAPOJENIA CISCO AKADÉMIE

Súčasťou bakalárskej práce je simulácia učebne Cisco akademie. Ako simulačný nástroj mal byť použitý už spomýnaný Packet tracer. Cieľom projektu je premietnuť učebňu, so všetkými jej súčasťami, do programu, v ktorom bude v maximálnej možnej miere funkčná tak ako reálna učebňa. To znamená konfiguráciu zariadení, pracovných staníc a spojovanie prvkov. V praxi si užívateľ – v tomto prípade študent – stiahne simuláciu ako súbor a spustí v programe Packet tracer. Súbor bude obsahovať všetko potrebné, aby práca zodpovedala práci v skutočnosti. Študenti budú môcť testovať rôzne zapojenia a konfigurácie bez rizika poškodenia, alebo znehodnotenia sieťových prvkov. Cieľom však nie je vytvoriť náhradu za cvičenia, ale doplnok, upevňujúci poznaky o zariadeniach Cisco, ich nastavení, spojovaní a najmä o fungovaní počítačovej siete v učebni.

Mojou úlohou bolo práve takýto súbor vytvoriť a pripraviť na nasadenie do výuky predmetu. Simulácia okrem iného demonštruje výhody, ktoré testovanie na virtuálnej sieti a až následná implementácia do reálne prináša.

Práca na prenesení Cisco učebne do programu spočíva v analýze možností, ktorými Packet tracer disponuje, a ich zúžitkovaní pri tvorbe simulácie. V priebehu práce bolo nutné vysporiadať sa s niektorými menšími nedostatkami programu a riešiť ich obkľukou cez spojenie viacerých funkcií dokopy. Prvé významné rozhodnutie predstavovalo to, že v simulácii bude použitý nástroj programu Packet tracer – Activity wizard.

### 7.1 Hľadanie vhodného riešenia

Ako som sa už zmienil, projekt je vytvorený v programe Packet tracer pomocou súčasti Activity wizard. Dôvod realizácie učebne pomocou tohto nástroja je, že oproti obvyčajnej simulácii dokáže zakázať fyzickú manipuláciu so zariadeniami a zobrazovať informačné popisky, ktoré uľahčujú orietáciu v simulovanej učebni. Vďaka blokovaniu pusúvania zaradení, odpadá starosť o rozhádzanie rozloženia a tým aj

prehľadu. Samozrejeme niekomu preddefinované rozloženie nemusí vyhovovať, prípadne sa môže stať, že uzamknutý prvok prekáža. Preto som sa snažil topológiu po fyzickej stránke optimalizovať a vyhnúť sa tak spomínaným problémom.

Učebňa v simulácii zachycuje pohľad na pôdorys tej reálnej (obr. 7.1). Orientácia korešponduje s prezentovanými obrázkami na stránkach predmetu. Hrubé rozloženie učebne je do farebných blokov.

Bloky s žltým pozadím reprezentujú celkovo tri rady s počítačmi, plus jeden blok figuruje ako stôl učiteľa.

Červený blok v pravej časti je oblasť, v ktorej sa nachádzajú sieťové zariadenia – smerovače a prepínače. Farebné bloky sú použité najmä kvôly prehľadnosti. Celkovo je v miestnosti 28 počítačov, z toho dva slúžia vyučujúcemu. Z týchto dvoch je využívaný iba jeden. Počty počítačov v radách simulovanej učebne korešpondujú s počtami v reálnej učebni. V tomto bode nastal prvý problém, pri vypracovávaní projektu simulácie učebne Cisco akademie.



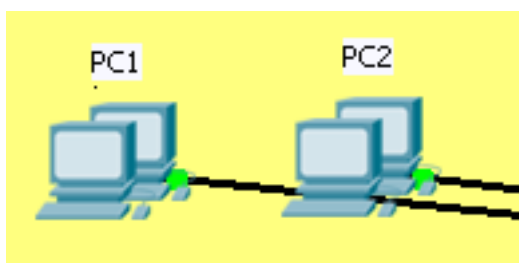
Obr. 7.1: Topológia Cisco učebne s 28 počítačmi a 3 stojanmi.

## 7.2 Simulácia reálnych počítačov

V reále obsahujú počítače dve sieťové karty a jeden sériový port. Takáto konfigurácia v Packet tracery nie je bohužiaľ možná. Problém sa nachádza v počte kariet, ktoré môže jedno koncové zariadenie obsahovať. V simulačnom prostredí je to iba jedna karta, respektíve jeden slot. V slote môže byť jeden modul. Na výber sú dva.



Ethernetový port a bezdrôtový adaptér. Použitie iba jedného modulu by nezodpovedalo skutočnosti. Riešenie problému som sa pokúsil najprv hľadať v nasadení rozdielneho zariadenia. Do úvahy pripadal server, ktorý by vo finále figuroval ako pracovná stanica. Realizácia však stroskotala na rovnakom, vyššie uvedenom, probléme. Ako najideálnejšie východisko sa javí duplikácia všetkých koncových staníc. To znamená, že jednu reálnu stanicu v simulácii reprezentujú dve s podobnou konfiguráciou. V prostredí som sa snažil zariadenia, ktoré sú spolu brané ako jeden počítač, umiestniť navzájom čo najbližšie, však tak, aby si nezavadzali. Výsledok je zreteľný z obrázku obr. 7.2 . Počítače ležia jeden na druhom. Vrchný počítač figuruje ako ethernetová sieťová karta do Internetu a VUT siete. Prekrývaný počítač reprezen-



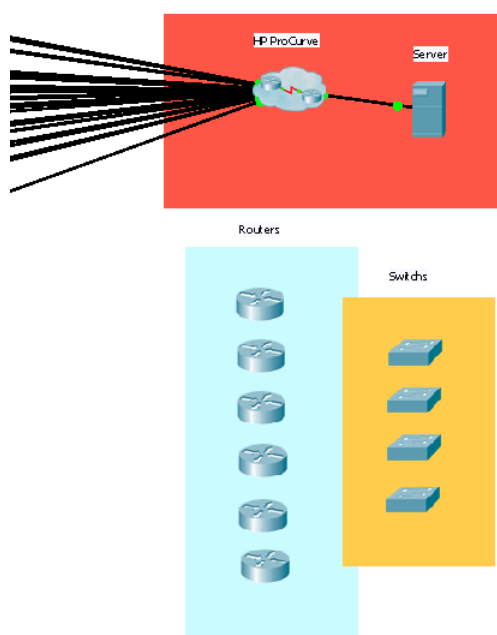
Obr. 7.2: Počítač „maskovaný“ dvoma koncovými zariadeniami.

tuje sieťový adaptér pre prístup do testovacej siete používanej vo výuke. Dôležité bolo nájsť logické pomenovanie staníc, aby nenastal zmätok. Na pomenovanie staníc pripojených do VUT siete aplikujem systém mien vo formáte „PCx realNet“ a staníc pripojených do výukovej siete „PCx testNet“. Písmeno „x“ reprezentuje číslo stanice. Čísla korešpondujú s číslami vo všetkých ostatných materiáloch. Teda na príklad počítač v učebni pod označením 13, odzrkadluje v simulačnom prostredí koncové stanice „PC13 realNet“ a „PC13 testNet“.

Tretie – sériové rozhranie sa vďaka zdvojeniu nachádza na počítači 2-krát. Použitie tohoto rozhrania považujem za diskutabilné, pretože na rozdiel od reálnej situácie, kde je nutnosťou spojenie cez konzolu, nastavovanie zariadení prebieha priamo bez nutnosti spojenia počítača a sieťového prvku. Aj keď táto možnosť nebude pravdepodobne patriť k najvyužívanejším, jej použitie nie je zakázané, ani obmedzené.

## 7.3 Stojany – racky, smerovače a prepínače

Ako už bolo spomenuté, v červenej oblasti sa nachádzajú sieťové zariadenia. Aby ostala previazanosť so skutočnou miestnosťou, podlieha tiedenie smerovačov a prepínačov rovnakému systému, čo znamená umiestnenie do troch stojanch – racky. V simulácii sa na združovanie zariadení používajú tzv. clustre. Ide o nástroj vytvarajúci prostredie so stromovou štruktúrou. Použitie sa vyplatí najmä v topológii s veľkým množstvom zariadení, čo topológia Cisco akademie je. Každý cluster je pomenovaný podľa stojanu, ktorý reprezentuje. Po rozkliknutí sa zobrazí obsah clusteru a teda aj vstúpi do nižšej úrovne. Clustre zahŕňajú práve toľko sieťových prvkov, koľko stojany v učebni. Farebné bloky triedia zariadenia do častí so prepínačmi a smerovačmi. Prvý cluster – stojan okrem klasickej výbavy, v podobe smerova-



Obr. 7.3: Prvý stojan s prepínačom HP ProCurve a serverom.

čov a prepínačov, obsahuje server a ďalší cluster. Server má funkciu najmä DHCP servera. Priraduje IP adresy staniciam pripojeným do ostrej siete z rozsahu adries 147.229.0.0/16 tak, ako v skutočnosti. Ďalšie služby typu web server, alebo Trivial File Transfer Protocol (TFTP) server sa v cvičeniach veľmi nepoužívajú, avšak konfigurácia nie je problém a je povolená. Druhým zvláštnym prvkom nachádzajúcim

sa v prvom stojane je cluster s názvom HP ProCurve. Funkcia zariadenia spočíva v spojení všetkých staníc označených „PCx realNet“ do jednej siete, ktorú obsluhuje už spomínaný DHCP server. Cluster maskuje dva prepínače obr. 7.3, aby navonok figurovali ako jeden veľký. K spomínanému riešeniu som bol nutný pristúpiť, pretože ani jedno z ponúkaných zariadení, nemá dostatočný počet portov k obsluhu 28 staníc. Prepínač s najväčším počtom ethernetových rozhraní ich obsahuje len 24. Použité sú preto dva Cisco prepínače s typovým označením C2940-24TT. Zariadenia s už zmieneným typovým označením obsahujú aj všetky ostatné clustre, ako prepínače používané pri cvičeniach. Zhoda so skutočnou učebňou existuje aj v tomto bode.

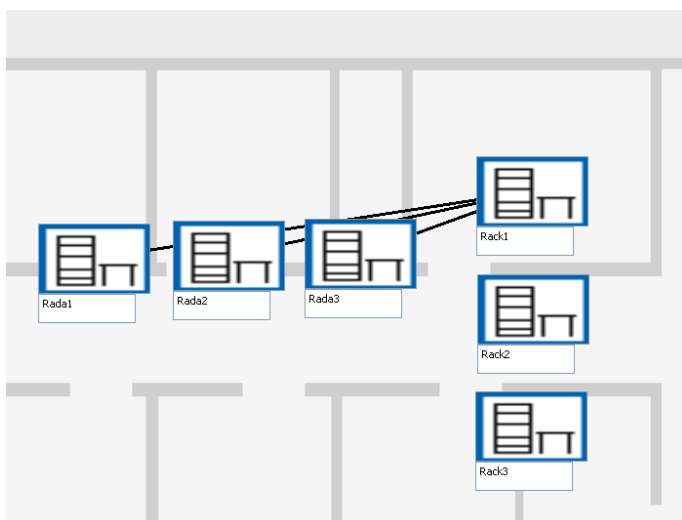
Ďalej som do simulácie použil smerovače s označením C2811. Základný model tohoto typu nebolo vhodné použiť, pretože neobsahoval dostatočné množstvo, ako sériových, tak aj ethernetových rozhraní. Packet tracer ponúka širokú paletu rozširujúcich modulov, z ktorých vybrať ten správny nepredstavuje veľký problém. Smerovač som rozšíril celkovo o tri moduly. Najväčší z nich rozmnožil ethernetové porty, nutných k pripojeniu smerovačov prípadne priamo staníc. Počet sériových rozhraní znásobili zvyšné dva moduly. Samostatný smerovač v základnom prevedení neobsahoval žiadny. Teoreticky je možná náhrada za ethernetové porty, ale vzhľadom na rozšírenosť použitia sériových rozhraniach v cvičeniach, by riešenie bolo kontraproduktívne. Teda vo finále má smerovač štyri sériové linky, tri ethernetové porty a dve rozhrania na administratívnu činnosť (konzolový a AUX vstup/výstup).

Zaujímavou komponentou Packet traceru je zobrazenie nie len logickej štruktúry, v ktorej prebieha väčšia časť práce, ale aj fyzická organizácia zariadení. Vo väčšine sú obidve zobrazenia takmer zhodné. V prípade Cisco akadémie môžeme konštatovať, že navrhnutá logická topológia je takmer rovnaká ako fyzická.

## **7.4 Fyzické rozloženie zariadení v prostredí Packet tracer**

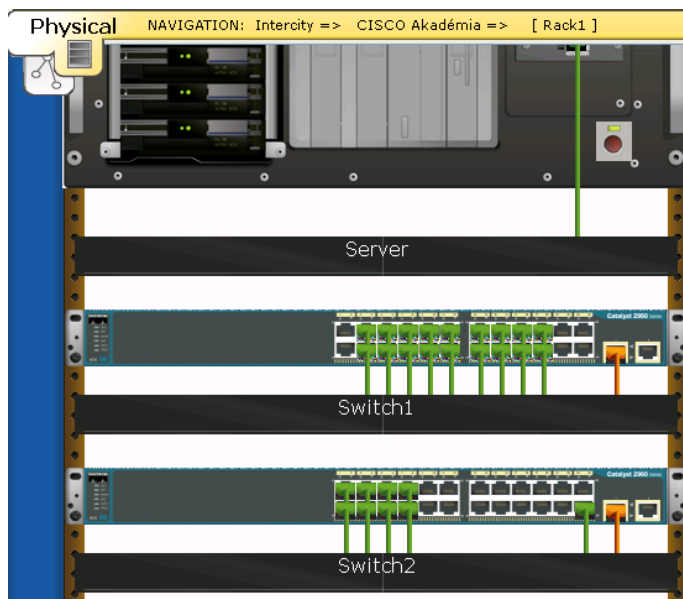
Prepínanie medzi zobrazeniami prebieha cez menu v hornej časti obrazovky. Fyzická topológia má, podobne ako logická, hierarchickú štruktúru. Najvyššiu úroveň reprezentuje učebňa Cisco akadémie. V nižšej úrovni sa už dostávame na stupeň,

v ktorom už figurujú rady s počítačmi a stojany (obr. 7.4). Po rozkliknutí ktoréhokoľvek prvku sa zobrazia samotné zariadenia. Samozrejeme, že podľa prvku (stojanu,

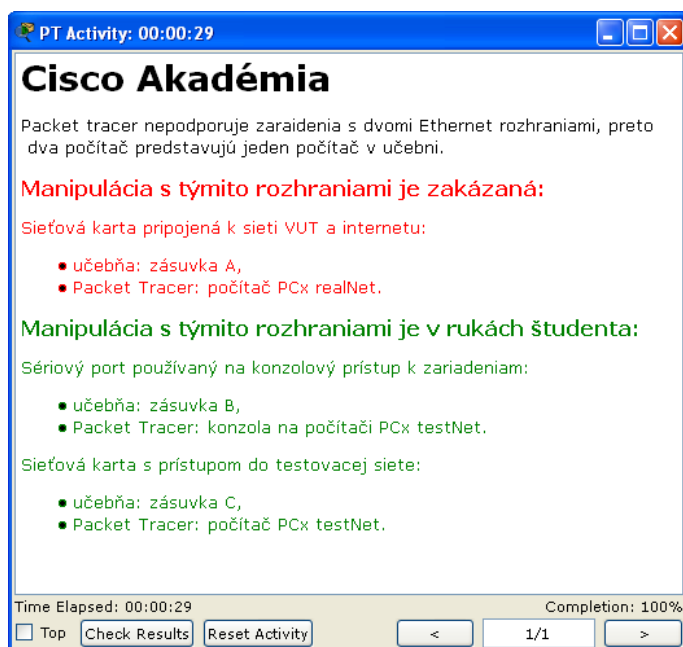


Obr. 7.4: Uroveň v ktorej vidieť stojany a rady.

rady) dostaneme zariadenia príslušiace k stojane či rade. To znamená, že v prípade rady sú za sebou zachytené všetky počítače jej príslušiace. Rozkliknutie stojanu nározorne vyobrazí sieťové prvky ako v reálnej situácii a to i s kabelážou (obr. 7.5). Operácie spracovávané na tejto úrovni sú mierené najmä na správu napájania a sieťovej kabeláže. Súčasťou simulácie je aj informačné okno (obr. 7.6). Editácia publikovaných inforácií prebieha cez jednoduchý HyperText Markup Language (HTML) editor. Využívať je možné základné značky – tagy. Do informácii som zahrnul základné inštrukcie a pokyny analogické s direktívami platnými v Cisco učebni. Súbor so simulovanou učebňou by mal byť stiahnuteľný z E-Learningu VUT. Súčasťou je i webová prezentácia, ktorá informuje o základnom ovládaní a navigácii v programe Packet tracer a simulácii.



Obr. 7.5: Grafické znázornenie zariadení a ich zapojenia.



Obr. 7.6: Informácie zobrazované pri každom spustení úlohy.

## 8 ZÁVER

Cieľ bakalárskej práce bol rozdelený do dvoch projektov. Prvý mal za úlohu premietnuť učebňu Cisco akadémie, v ktorej prebieha výuka predmetov MCA a BCA, do programu na simuláciu počítačových sietí – Packet tracer a druhý vytvoriť vypracovateľnú úlohu na zvolené téma do týchto predmetov. Nakoniec bolo nutné pripraviť k týmto projektom webovú prezentáciu so základnými údajmi o jednotlivých súboroch, ktoré by mali byť prístupné v eLearningu VUT.

Môžem konštatovať, že Packet tracer je zaujímavý simulačný nástroj. Ideálny k osvojeniu si základných princípov komunikácie v sieti a konfiguračných postupov s Cisco zariadeniami. Vo svojej práci som sa snažil využiť všetky jeho klady. Výsledkom snaženia sú dva projekty, ktoré majú potenciál stať sa súčasťou prípravy na predmety MCA a BCA.

Prvý z nich – simulácia učebne, vytvára ideálne prostredie na testovanie laboratórnych úloh, pretože zahŕňa všetky prvky vyskytujúce sa v miestnosti. Študenti sa budú môcť zoznámiť sa s úlohami skôr, ako ju začnú zapájať a nastavovať v reálnej sieti.

Za tému druhého projektu som si vybral smerovací protokol OSPF. Výsledná úloha je spracovaná v nástroji Activity wizard. Tým som mal možnosť implementovať dôležité súčasti, ako napríklad informačné okno a automatické vyhodnotenie. Myslím, že tým sa potenciál úlohy zvýšil a môže byť zaradená do prípravy na predmety MCA a BCA.

Prácou som sa snažil zároveň predstaviť výhody a možnosti simulačného nástroja Packet tracer. Potencál úloh, vytvorených týmto programom, nekončí iba v predmete MCA a BCA, ale majú šancu byť využité aj v iných predmetoch, pretože dokážu názorne ukázať fungovanie počítačových sietí.

# LITERATÚRA

- [1] *Cisco Akademie* [online]. 2008 [cit. 28. 11. 2008]. Český. Dostupný z WWW: <[http://adela.utko.feec.vutbr.cz/cisco\\_akademie/](http://adela.utko.feec.vutbr.cz/cisco_akademie/)>.
- [2] GRYGAREK, P. *Směrování v počítačových sítích a v Internetu* [online]. 2006 [cit. 12. 10. 2008]. Dostupný z WWW: <<http://www.cs.vsb.cz/grygarek/SPS/lect/routingucitele.pdf>>.
- [3] SPORTACK, MARK A. *Směrování v sítích IP* [preklad Krásenský, D.]. 1. vydanie. Brno : Computer Press, 2004. 351 s. ISBN 80-251-0127-4.
- [4] DROMS, R., LEMON, T. *DHCP Příručka administrátora* [preklad Blažík, M., Černý, J.]. 1. vydanie. Brno : Computer Press, 2004. 490 s. ISBN 80-251-0130-4
- [5] EMPSON, S. *CCNA : kompletní přehled příkazů : autorizovaný výukový průvodce* [preklad Krásenský, D.]. 1. vydanie. Brno : Computer Press, 2009. 336 s. ISBN 978-80-251-2286-0.
- [6] GRAZIANI, R., JOHNSON, A. *Routing Protocols and Concepts, CCNA Exploration Companion Guide*. Cisco Press, USA, 2007. 606 s. ISBN 978-1-58713-206-3.
- [7] HUCABY, D., MCQUERRY, S. *Konfigurace směrovačů Cisco*. [preklad Veselký, J.]. Computer press, 2004. 632 s. ISBN 80-722-6951-8.
- [8] KRČMÁŘ, P. *Linux : postavte si počítačovou síť* 1. vydanie. Praha : Grada, 2008. 182 s. ISBN 978-80-247-1290-1
- [9] *Směrovací protokol OSPF* [online]. 2004 [cit. 11. 12. 2008] Dostupný z WWW: <<http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html>>.
- [10] *Packet Tracer 5.0 Data Sheet* [online]. ©2008 [cit. 5. 12. 2008]. Angličtina. Dostupný z WWW: <[http://cisco.netacad.net/cnams/resourcewindow/noncurr/downloadTools/app\\_files/PT5\\_0\\_DS.pdf](http://cisco.netacad.net/cnams/resourcewindow/noncurr/downloadTools/app_files/PT5_0_DS.pdf)>.

- [11] PRITSKY, T., MOORE, M., SOUTHWICK, P., RIGGS, C. *Telecommunications: a beginner's guide*. McGraw-Hill Professional, 2001. 507 s. ISBN 978-00-721-9356-5



# **ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK**

ARP Address Resolution Protocol

AUX Auxiliary – pomocný port

BDR Backup Designated Router – záložný referenčný router

BCA CISCO akadémia – bakalársky program

CCNA Cisco Certified Network Associate

CLI Command-line interface – príkazový riadok

DBD Database Description

DHCP Dynamic Host Configuration Protocol

DR Designated Router – referenčný router

HTML HyperText Markup Language

IETF The Internet Engineering Task Force

IGP Interior Gateway Protocol

IOS Internetwork Operation System

IP Internet Protocol

IPv4 Internet Protocol version 4

LAN Local Area Network

LSA Link State Advertisement

LSAck Link State Acknowledgement

LSP Link State Packets

LSR Link State Request

LSU Link State Update

MAC Media Access Control

MCA CISCO akadémia – magisterský program

NBMA Non–Broadcast Multiple Access

NAT Network Address Translation

OS operačný systém

OSI Open Systems Interconnection

OSPF Open Short Path First

OSPFv2 Open Short Path First version 2

RIP Routing Information Protocol

SPF Shortest Path First

SSH Secure Shell

TCP/IP Transmission Control Protocol / Internet Protocol

Telnet Telecommunication Network

TFTP Trivial File Transfer Protocol

TTL Time To Live

VUT Vysoké učení technické

Wi-Fi Wireless Fidelity

# ZOZNAM PRÍLOH

<b>A</b>	<b>CD-ROM</b>	<b>43</b>
A.1	BP_xwolfj01.pdf . . . . .	43
A.2	cisco_class.pka . . . . .	43
A.3	cisco_exam.pka . . . . .	43
A.4	class_web.html . . . . .	43
A.5	exam_web.html . . . . .	43
A.6	styles.css . . . . .	43
A.7	Zložka: pic . . . . .	44

## **A CD-ROM**

### **A.1 BP\_xwolfj01.pdf**

Elektronická verzia bakalárskej práce vo formáte PDF

### **A.2 cisco\_class.pka**

Súbor programu Packet tracer obsahujúci simuláciu Cisco akademie. Vytvorené a testované na verzii 5.1. Otvorenie súboru prebieha štandardným spôsobom cez menu v okne programu.

### **A.3 cisco\_exam.pka**

Súbor programu Packet tracer obsahujúci vypracovateľnú úlohu s OSPF smerovací protokolom. Vytvorené a testované na verzii 5.1. Otvorenie súboru prebieha štandardným spôsobom cez menu v okne programu.

### **A.4 class\_web.html**

Webová prezentácia pre simuláciu učebne Cisco akademie vo formáte HTML.

### **A.5 exam\_web.html**

Webová prezentácia pre vypracovateľnú úlohu s OSPF smerovací protokolom vo formáte HTML.

### **A.6 styles.css**

Štýlový css súbor pre HTML prezentácie.

## **A.7 Zložka: pic**

Zložka obsahujúca obrázky k webovým prezentáciám.